UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/665,627	09/19/2000	Jean-Francois Le Pennec	909.0030USU	5560

7590 03/18/2004

Harry F Smith Esq
Ohlandt Greeley Ruggiero & Perle LLP
One Landmark Square
Stamford, CT 06901

EXAMINER	
QUINONES, EDEL H	
ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 03/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

9

Office Action Summary	**Application No.** 09/665,627	**Applicant(s)** LE PENNEC ET AL.
	Examiner Edel H Quinones	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _19 September 2000_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-22_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-22_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _19 September 2000_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _4_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

III. Detailed Action

1. Claims 1-22 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement filed on 12/26/2000 complies with the provisions of MPEP § 609. It has been placed in the application file, and the information referred to therein has been considered as to the merits.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 3, 4, 7, 9, 11-18 and 21-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Touboul et al. (U.S. Patent 6,154,844 and Touboul hereinafter).

In regards to claim 1, Touboul teaches a method, for use in a virus-free certificate authority (i.e. inspector) (figure 1, item 100), of generating a virus-free certificate (figure 1, item 170) certifying that a file (i.e. downloadable) is virus-free (col. 5, lines 52-53) comprising the steps of:

- receiving a virus-free certificate request for a file from a server or a client system (i.e. developer) (figure 1, item 120), said virus-free certificate request comprising the file for which the virus-free certificate is requested (figure 7, step 705). (The Examiner infers that the action of sending a file to the inspector is an implied request for a virus inspection);
- determining whether a virus-free certificate is integrated in the file (figure 7, step 720);

If no virus-free certificate is integrated in the file (figure 7, step 720):

- determining whether the file is virus-free or not (figure 7, steps 750 and 755) (col. 10, lines 5-7);

if the file is declared virus-free by the virus-free certificate authority (figure 7, step 760):

- generating a virus-free certificate comprising a file signature for certifying that said file is declared virus-free by the virus-free certificate authority (figure 6, step 635 performed during step 750 in figure 7);
- integrating the generated virus-free certificate in the file (figure 6, step 635 performed during step 750 in figure 7);

- sending back in response to the virus-free certificate request the file with the integrated virus-free certificate (figure 7, step 770).

In regards to claim 3, Touboul teaches that the file comprised in the virus-free certificate request contains an integrated virus-free certificate (figure 7, step 725).

In regards to claim 4, Touboul teaches the steps of:

If the file comprises an integrated virus-free certificate, determining whether the virus-free certificate integrated in the file has been previously generated by the virus-free certificate authority, and if that is the case (i.e. "YES" branch in figure 7, step 720), updating the virus-free certificate (figure 7, step 725).

If the virus-free certificate integrated in the file has not been previously generated by the virus-free certificate authority, then generating a new virus-free certificate (i.e. "NO" branch in Figure 7, step 720 followed by step 750).

That is, Toubol teaches that the network system may include multiple inspectors (i.e. certification authorities), wherein each inspector may provide a different content inspection. Each inspector would attach a corresponding DSP and a certificate verifying the authenticity of the attached DSP (col. 5, lines 48-55). Thus, it can be inferred that if the inspector that originally produced the certificate receives a downloadable with an integrated certificate, the certificate is updated (i.e. authenticated). But if an inspector different from the one that originally produced the certificate receives it, the downloadable is inspected and a new certificate is attached to it.

In regards to claim 7, Touboul teaches that the step of determining whether the file is virus-free or not comprises the further step of executing one or a plurality of anti-virus programs on said file for detecting viruses (col. 9, lines 12-17).

In regards to claim 9, Touboul teaches that the virus-free certificate further comprises:

a file identification (i.e. Downloadable ID) (col. 6, lines 6-7);

a virus-free certificate authority identification (i.e. name of the certifying authority that issued to certificate) (col. 6, lines 12-13);

a public key for decrypting the file signature (i.e. the inspector's public key) (col. 6, line11);

Touboul does not teach that the virus-free certificate also comprises a certificate signature for authenticating purposes. However, the use of a certificate signature for authenticating a certificate is old and well known in the art. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to include a certificate signature with the certificate because this would provide a recognized way of authentication.

In regards to claim 11, Touboul teaches that the step of generating a file signature comprises the further steps of:

- hashing the file to generate a file digest (i.e. Downloadable ID) (col. 8, lines 61-63);
- encrypting the file digest (i.e. Downloadable ID) using a private key (col. 6, line 5).

In regards to claim 12, the claim limitation recites a system implementing a virus-free certificate authority comprising a processor that executes a program for implementing a method substantially similar to the method of claim 1, therefore the same rejection applies.

In regards to claim 13, the claim limitation recites a computer program recorded on a computer-readable medium and comprising instructions executing a method substantially similar to claim 1, therefore the same rejection applies.

In regards to claim 14, Touboul teaches a method, for use in a server or client system (figure 1), of determining that a file is virus-free (col. 1, lines 26-27) comprising the steps of:

- determining whether a virus-free certificate is integrated within a file (figure 7, step 720);

if a virus-free certificate is integrated within the file:

- authenticating the virus-free certificate(figure 7, step 725), said virus-free certificate comprising a certificate signature (col. 6, lines 10-13);
- authenticating the file (figure 7, step 735), said virus-free certificate comprising a file signature (i.e. Downloadable ID), said file signature certifying that said file has been declared virus-free by a virus-free certificate authority (i.e. each inspector would attach a corresponding DSP and a certificate verifying the authenticity of the attached DSP) (col. 5, lines 52-54).

In regards to claim 15, Touboul teaches that the step of authenticating the file comprises the further steps of:

- decrypting the file signature (i.e. Downloadable ID) using a public key comprised in the virus-free certificate (col. 9, lines 36-41).
- hashing the file to generate a file digest (col. 9, lines 44-45);
- comparing the decrypted file signature with the generated file digest (col. 9, lines 49-52).

In regards to claim 16, Touboul teaches that the step of authenticating the virus-free certificate comprises the further step of validating the virus-free certificate. That is, Touboul teaches that the virus-free certificate may include an expiration date (col. 6, lines 11). Therefore, it can be inferred that the step of authenticating the virus-free certificate may include not only the authenticating of the Downloadable ID (col. 9, line37-40), but also the validating of the expiration date.

In regards to claim 17, Touboul teaches that the step of validating the virus-free certificate comprises the further step of:

- determining whether the virus-free certificate is valid or not, as discussed for claim 16 above;

If the virus-free certificate is not valid (figure 7, step745):

- requesting a virus-free certificate update or an updated virus-free certificate update to a virus-free certificate authority (figure 7, step 750).

In regards to claim 18, Touboul teaches that the virus-free certificate further comprises:

a file identification (i.e. Downloadable ID) (col. 6, lines 6-7);

a virus-free certificate authority identification (i.e. name of the certifying authority that issued to certificate) (col. 6, lines 12-13);

a public key for decrypting the file signature (i.e. the inspector's public key) (col. 6, line11);

In regards to claim 21, the claim limitation recites a system implementing a virus-free certificate authority comprising a processor that executes a program for implementing a method substantially similar to the method of claim 14, therefore the same rejection applies.

In regards to claim 22, the claim limitation recites a computer program recorded on a computer-readable medium and comprising instructions executing a method substantially similar to claim 14, therefore the same rejection applies.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 2, 5-6, 8, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Touboul in view of Hailpern et al. (U.S. Patent 6,275,937 and Hailpern hereinafter).

In regards to claim 2, Touboul teaches the system of claim 1 as discussed above.

Touboul does not teach that the virus-free certificate request comprises a list of one or a plurality of anti-virus programs to execute on the file to determine whether the file is virus-free or not.

Hailpern discloses a collaborative method of virus checking data object in a network of servers (col. 1, lines 25-27).

Hailpern teaches including within a virus-free certificate request (i.e. PRRR) a list of one or a plurality of anti-virus programs to execute on a file to determine whether the file is virus-free or not (col. 9, lines 61-63), (col. 10, lines 37-67).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Touboul with the teachings of Hailpern to include within a virus-free certificate request a list of one or a plurality of anti-virus programs to execute on a file to determine whether the file is virus-free or not with the motivation to establish a collaborative method for processing the files (Hailpern, col. 3, lines 65-66).

In regards to claim 5, Touboul does not teach that the file further comprises a file header comprising:

- a non encrypted file signature;
- a file length;
- a product name.

Hailpern teaches a file (i.e. http request/response) comprising a file header comprising:

- a non encrypted file signature (figure 10, step 7020);
- a file length (col. 2, line 15);
- a product name (i.e. information or data associated with a given object) (col. 2, line 10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Touboul with the teachings of Hailpern to include that the file further comprises a file header comprising a non encrypted file signature, a file length; and a product name with the motivation to establish a collaborative method for processing the files (Hailpern, col. 3, lines 65-66).

In regards to claim 6 and 19, Touboul teaches that the step of integrating the virus-free certificate in the file comprises the further step of:

- appending the virus-free certificate to the file (figure 6, step 635).

Touboul does not teach the additional steps of:

- modifying the file header, preferably:
    - the non encrypted file signature;

- o the file length;
- o a product name, said product name comprising means for identifying the integrated virus-free certificate.

Hailpern teaches the updating of header fields as a result of the modification of a data object (i.e. the PJ.Header is modified, if necessary, to reflect the new, processed data [e.g. the value of the "length" field may have changed due to modifications made to the data objects by one or more of the processes, such as IBM Antivirus]) (col. 17, lines 14-19). The Examiner infers that likewise, the other affected fields in the header (i.e. file signature and product name) are also updated.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Touboul with the teachings of Hailpern to include the additional steps of modifying the file header, preferably the non encrypted file signature; the file length; and a product name comprising means for identifying the integrated virus-free certificate with the motivation to establish a collaborative method for processing the files (Hailpern, col. 3, lines 65-66).

In regards to claim 8, Touboul teaches the system of claim 1 as discussed above.

Touboul, however, does not teach that the virus-free certificate further comprises a list of the anti-virus programs that have been executed on the file.

Hailpern discloses a certificate (i.e. listing of the results of applying anti-virus checking) (col. 13, line 29) comprising a list of the anti-virus programs that have been executed on a file (col. 13, lines 30-36).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Touboul with the teachings of Hailpern to include that the virus-free certificate further comprises a list of the anti-virus programs that have been executed on the file with the motivation to establish a collaborative method for processing the files (Hailpern, col. 3, lines 65-66).

In regards to claim 20, Touboul teaches the method of claim 14.

Touboul does not teach that the step of determining whether a virus-free certificate is integrated within a file comprises the further step of determining whether a product name within a file header comprises means for identifying the integrated virus-free certificate.

Hailpern teaches that a product name within a file header comprises means for identifying the integrated virus-free certificate (i.e. a PICS Processing Label is a conventional PICS Label which allows servers having features of the current invention to indicate the processing they have applied to a piece of data they return or transfer by including the label in the HTTP header as an additional field) (col. 12, lines 50-54) (col. 13, lines 28-36).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Touboul with the teachings of Hailpern to include that the step of determining whether a virus-free certificate is integrated within a file comprises the further step of determining whether a product name within a file header comprises means for identifying the integrated virus-free certificate with the motivation to establish a collaborative method for processing the files (Hailpern, col. 3, lines 65-66).

6. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Touboul in view of Wiener et al. (US 20030110376 A1 and Wiener hereinafter).

In regards to claim 10, Touboul teaches the system of claim 1 as discussed above.

Touboul does not teach the further steps of:

- identifying the server or client system where the file comprising the integrated virus-free certificate is stored;
- updating the file with the integrated virus-free certificate.

Wiener discloses a system for providing certificate lifetime data (see Abstract).

Wiener teaches identifying a server or client where are file comprising a certificate is located and updating the file with the certificate (i.e. after the manager 12 has received the new digital signature key pair from the client unit, the manager 12 creates a new digital signature certificate containing the selected public key expiry data as entered by the security officer, for the client generating the digital signature key pair update request. The manager 12 associates the selected expiry data with the new key pairs as indicated by linking the selected expiry data with the public digital signature key as shown in block 46. The manager sends the new digital signature certificate to the requesting client on the secure online path) (see par. 0022).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Touboul with the teachings of Wiener to include the additional steps identifying the server or client system where the file comprising the integrated virus-free certificate is stored; updating the file with the integrated virus-free certificate with the motivation to establish a method of updating certificates that is effectively transparent to a user (Wiener, par. 0006).

Other Prior Art Made of Record

7. A. Waldin et al. (U.S. Patent No. 6,094,731) discloses an antivirus accelator for computer networks;

B. Chang et al. (U.S. Patent No. 5,724,425) discloses a system and method for enhancing software security and distributing software;

C. Rubin (U.S. Patent No. 5,638,446) discloses a method for the secure distribution of electronic files in a distributed environment;

A. Houser et al. (U.S. Patent No. 5,606,609) discloses an electronic document verification system and method;

B. Murray (U.S. Patent No. 6,321,333) discloses efficient digital certificate processing in a data processing system; and

C. Koehler (U.S. Patent No. 6,301,658) discloses a method and system for authenticating digital certificates issued by an authentication hierarchy.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Points of Contact

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edel H. Quiñones whose telephone number is 703-305-8745. The examiner can normally be reached on M-F (8:00AM-5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Edel H. Quiñones
Patent Examiner
Technology Center 2100

March 15, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100